Bitcoin, Blockchains, and Beyond

Matthew Foster, Caleb Mennen, Jared Smith

University of Tennessee, Knoxville

rfoste11@vols.utk.edu, cmennen@vols.utk.edu, jms@vols.utk.edu

Contents

Abstract

In this paper we present a study of

I. Introduction

The concept of Bitcoin was presented to the world in a whitepaper by Satoshi Nakamoto on October 31, 2008. A note was a posted to the Cryptography Mailing List the following day, which contains the abstract from the whitepaper. This was followed up in 2009 with the release of the Bitcoin open source software. So, what is Bitcoin? Bitcoin represents one of several steps in the development of a crypto-currency. It is significant in that it attempts to solve two problems associated with decentralized crypto-currencies: the Byzantine Generals problem, which is a common problem in distributed systems, and the double spend problem. Bitcoin uses the concept of a blockchain in a peer-to-peer network in an attempt to solve these issues in a probabilistic manner. In this paper we are going to provide an overview of Bitcoin, then take a deeper look at the mathematics and cryptography behind Bitcoin. We will also discuss Bitcoin wallets and Bitcoin mining. We will then look into some of the alternative crypto-currencies to Bitcoin and finally look into some intriguing applications of blockchains.

II. Overview

Satoshi Nakamoto outlined some of the reasons for creating Bitcoin in his whitepaper. Bitcoin was created as an alternative to the existing centralized financial institutions. Satoshi believed that there were several problematic aspects to the current centralized system. The Bitcoin vision was to have a distributed, decentralized crypto-currency. It was to be based on, "cryptographic proof instead of trust". With Bitcoin, there would be no need for a trusted third party. The weight of a peer-to-peer distributed network would serve as a means to record all transactions and protect users from the double-spending problem. Bitcoin was created as open source software, and the code resides on Github. Anyone interested can see the code.

How does Bitcoin work? A transaction in Bitcoin starts with a wallet, from which you can create an account and have a place to perform transactions. There are several different kinds of wallets, but they all allow you to perform the same core actions. The process starts when you create an account with your wallet. Once your account is established, you will be able to perform transactions on the Bitcoin network. Assuming you have Bitcoin to spend and you want to transfer some Bitcoin to another account, you create a transaction by providing an account number to transfer the Bitcoin to along with the amount you want to transfer. Your wallet then broadcasts the transaction to the Bitcoin network. Eventually (in about 10 minutes) your transaction will be combined into a block (of other recently made transactions) which is then added to the blockchain.

Each transaction is distributed across all the computers participating in the Bitcoin network as part of the blockchain. The blockchain acts as the Bitcoin ledger. It is a chain of blocks that are linked in sequential order. A block is comprised of four parts: the size of the block, a block header, a transaction count, and a list of transactions in the block. The Block header is structured to include: a bitcoin version number (in case of a change in the blockchain), a double SHA256 hash of the previous block header, a hash of all transactions in the current block, a timestamp indicating when the block was created, the difficulty target for the block, and the nonce.

Anyone in the network can view the blockchain and see all of the previous transactions that have taken place. Current transactions are compiled every ten minutes or so into a block of transactions. The block is then finalized by a lucky bitcoin miner and added to the blockchain. This miner gets a bitcoin from the confirmation of the transaction and also pays the transaction fee. Because everyone on the Bitcoin network has access to a copy of the blockchain, it is difficult to change a transaction that has taken place. As a transaction settles deeper into the blockchain it becomes even harder.

This hardness as you go deeper and deeper into the layer of the blockchain can be thought of as a layer of thin ice over a much more permanent and deeper layer of hard ice that makes up the foundation. You can easily break the ice on top, but you cannot break and get through the hard, permanent ice underneath the first few layers of ice on top. This is analogous to the nature of the blockchain, where the thin layer on top are the last few most recent transactions that the entire community of Bitcoin users can change if transactions go wrong or more transactions are added. The deeper layers of ice are analogous to the deeper levels of the blockchain where transactions cannot be changed. This allows for a constant source of truth per transaction to be derived from the existing blockchain that can be used to reconcile discrepancies between individuals competing for mined bitcoins.

III. Mathematics and Cryptography

Bitcoin uses several different cryptographic algorithms, all of which have been in wide use for some time and are considered "safe" algorithms. Bitcoin uses one way functions, hash functions, elliptic curve cryptography, asymmetric key cryptography, and digital signatures. The specific hash functions used are SHA256 (Secure Hash Algorithm) and RIPEMD160 (Race Integrity Primitives Evaluation Message Digest). Bitcoin uses elliptic curves to create digital signatures, specifically the Elliptic Curve Digital Signature Algorithm (ECDSA).

In order for Bitcoin to work, it has to have a way of keeping everyone's account private and a means to authenticate transaction requests. In other words, Bitcoin must guarantee that your account will be secure and that there is a means in place for you to authorize the transactions you place. No one else should be able to access your accounts. The process begins with the creation of a public/private key pair. Your account number is derived from your public key.

Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA) to generate the public/private key and perform the signature process. There is a particular Elliptic curve that Bitcoin bases its cryptography on. We are not going into detail about how elliptic curves work, but do we need to mention some numbers related to the Elliptic Curve that Bitcoin uses. The curve is referred to by "secp256k1". We will now explore the mathematical and cryptographic properties of Bitcoin, notably the elliptic curve algorithm underneath and the verification of signatures by the algorithm.

- An elliptic curve is represented algebraically by the form: $Y2 = x3 + ax + b$, where a and b represent constants that define the curve.
- Bitcoin uses the curve defined by $a = 0$ and $b = 7$.
- The finite field (prime modulo) is represented by p.
- Bitcoin has chosen $p = 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1$.

- The finite field (prime modulo) is represented by p. The base point, G, represents the starting point on the elliptic curve. It is in the form $x, y)$.

- G is $G = 04\ 79BE667E\ F9DCBBAC\ 55A06295\ CE870B07\ 029BFCDB\ 2DCE28D9$ $59F2815B\ 16F81798\ 483ADA77\ 26A3C465\ 5DA4FBFC\ 0E1108A8\ FD17B448$ $A6855419\ 9C47D08F\ FB10D4B8$.

- The order, n, of the base point is $n = FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFE$ $BAAEDCE6\ AF48A03B\ BFD25E8C\ D0364141$.

- These numbers (p, a, b, G, n) are used by Bitcoin to calculate the public and private key and to sign transactions.

Given these numbers, now we can generate a private/public key (Barski, p. 154). First we generate a private key, d. It can be any integer between 1 and $(n - 1)$. Then, using the private key, d, we generate a public key, Q. The private key is multiplied by the generator point, G. To be clear, the multiplication used is Elliptic Curve multiplication, so the equation below is oversimplified. The general idea is that using elliptic curves, it is very easy to multiply the base point, G, by the private key, d, to come up with a public key, however it is very difficult to find the private key, d, from the public key, Q, and the base point, G. The public key, Q, will be in the form, (p, q), and $Q = dxG$. Once the key pair has been generated, we can sign transactions. To do this, we need the message (the transaction information) along with p, a, b, G, n, Q. Below are the steps involved in signing a transaction:

1. First calculate the hash of the message, h:
   $h\ =\ SHA256(message)\ mod\ n$

2. Choose a random integer, k, between 1 and $n - 1$.

3. Multiply $k \times G$ to calculate a point (r, t). This is more Elliptic Curve multiplication.

4. Find an s so that $s \times k(mod\ n)\ =\ (h + (r \times d))\ (mod\ n)$ and $(r,\ t) = kG$. $(r,\ s)$ represents the signature pair, which does not have to lie on the elliptic curve.

To verify the signature, you need (p, a, b, n, G, Q), the message, and (r, s). Anyone on the Bitcoin network will be able to access your public key, Q, the message (the transaction) and the signature (r, s). The other numbers are already available to everyone one the network. Others verify that you authorized the transaction, by checking to see if your signature is valid. If the signature matches, the rest of the network can be sure that it was your private key that signed the transaction. Only then will your transaction be added to the block of transactions. Here is the signature authorization process:

- First the hash of the message will be recalculated:
  $h \ = \ SHA256(message) \ (mod \ n)$
- Then the modular inverse of s must be found. It is represented by w:
  $w \ \times s \ (mod \ n) = 1$
- Calculate u:
  $u = h \ \times w \ (mod \ n)$
- Calculate v:
  $v = r \ \times w \ (mod \ n)$
- Calculate $(tx, \ ty)$:
  $(tx, \ ty) \ = \ uG + vQ$
- Finally, if $tx = r$, then the signature is valid.

One interesting note is that your public Bitcoin address is a double hash of your public key. Your address is created by running your public key through the SHA256 hash, and then through the RIPEMD160 hash. This sums up the cryptography involved in creating your Bitcoin address and public/private key pairs.

Hashing plays an important part in making a secure blockchain possible. When a block is added to the blockchain, the block is comprised of several sections. There is a group of transactions and a hash of the blockchain is included as well. By hashing the historical blockchain, it becomes very difficult to make any alterations to the blockchain. The way hash works is that it reduces a file into a number. Any changes in the file, no matter how small, will lead to a very noticeable change in the hash value. Since the blockchain is widely distributed on the Bitcoin network, anyone within the network can check the validity of a given blockchain.

IV. Bitcoin Wallet

The wallet is a piece of open source software that allows you to manage your Bitcoin accounts (Bitcoin addresses), and transfer money from one account to another. The Bitcoin address could be thought of as your public account number. You give this number to others so that they can transfer money into your account. They can't take money out of your account - only transfer money in. In addition to your Bitcoin address, you have private key. The private key allows you to authorize transactions from your account. It works like a PIN in the sense that you are the only person who knows your private number. If a transaction is signed with a private key, then it is assumed that the owner of the account has authorized the transaction. It is crucial that you do not lose your private key. The Bitcoin address and the private key are the only information tied to an account. There are no names or addresses associated with accounts and the private key can not be derived from the public address. If you lose your private key, there is no way to access the account tied to that public key.

V. Bitcoin Mining

An interesting use of cryptography can be found in Bitcoin mining. It revolves around the concept of proof of work. Proof of work means that you have to show that you have put effort into the Bitcoin system, before you "win" the right to add the block to the blockchain and the right to put your Bitcoin address as the recipient of new Bitcoins and transaction fees for the block. This shows that you have an investment in the system. Another system could be proof of 'investment'. With proof of work, you are putting 'sweat equity' into the system, and with proof of 'ownership' you are investing financial resources into the system. So how does a Bitcoin miner show proof of work? By doing a lot of computation.

So how does mining work? Miners have to hash a set of inputs, one of the inputs involves a guess. The output of this hash function has to be a number that lies below a given threshold (what is that threshold? How is it determined?) In order to find a number below the threshold, the miners guess a number and hash it along with the other provided criteria, then if it is not below the threshold, they guess another number, and so on. This amounts to enumerating through numbers, 'guessing' until an acceptable answer is found. Guessing is computationally expensive, but because hash functions are one way functions, guessing is ultimately cheaper than trying to reverse engineer an answer. When a miner guesses a correct value and shares it with the other miners, they are able to easily verify that the value is a correct value.

The transaction fees and release of a set amount of Bitcoin create the incentive to participate in Bitcoin mining. Participants are incentivized into using their CPU power to support the system rather than attack it. In theory the reward will be greater by supporting the system. It an attacker were able to out-compute the community of miners, the most that they could do is take back some of their payments (double spend). This path could lead to destabilizing the monetary system that they are trying to take advantage of. Of course, if they had the computing power to attack the system in such a way, they would have the power to âĂŸout-mine' others and earn Bitcoin in a way that would strengthen the value of their wealth.

VI. Bitcoin Alternatives

A unique aspect of Bitcoin that differentiates it from many other projects is the fact that it is open source. This has the implication, that not only can anyone see the code that underpins Bitcoin, but it allows anyone in the world to suggest changes or improvements to the Bitcoin protocols. The effect of this being, that the entire project has multiple eyes on it looking for potential flaws that could become problematic, and each proposed change gets the same thorough treatment before it goes live.

Due to the open source nature of Bitcoin, anyone can create a fork of the Bitcoin project, and make changes to create their own crypto-currency. A large number of systems exist like this, as modified forks off of the Bitcoin project. While there exist a large number of what are essentially Bitcoin clones, there are other non-Bitcoin crypto-currencies, often referred to as "altcoin" currencies, that are worth taking note of.

One such currency is Dogecoin. While it was gained it's spark of creation as a joke, referencing an image in online pop culture, it quickly distinguished itself from many other altcoins. One notable differentiating factor, is that it doesn't have a cap on how many Dogecoins may exist at any given time. While originally there was a cap of 100 billion, it was later removed. Another difference, is that the technology powering the proof-of-work algorithm to verify transactions is based on scrypt technology, or rather a password-based key derivation function. The importance of this, is many other altcoins can be mined using equipment that has been optimized in hardware for SHA-256. Due to the scrypt technology and how intensive it is on computer memory and computation time, it is impractical to make hardware-optimized equipment to rapidly mine Dogecoin.

An interesting aspect to Dogecoin is it's community. There are multiple instances in which the Dogecoin community has combined efforts to raise funds for various charities and notable causes. One such example is that during the 2014 Winter Olympics, the Jamaican Bobsled Team, while eligible to compete in the Olympics, were unable to afford the costs of attending the competition. Over the course of the fundraising campaign, approximately $130,000 had been raised, surpassing the goal of $40,000. Another altcoin with a sizable market share is Litecoin. While it was a fork of Bitcoin originally, and shares large similarities with Bitcoin, it has three key differences. One difference is that it is capped at 84 million litecoins, four times as many currency units than Bitcoin. Another is that, like Dogecoin, Litecoin uses scrypt for it's proof-of-work algorithm. Finally, the Litecoin network is geared towards processing a block every 2.5 minutes. The rationale is so that transaction confirmation is done more quickly than Bitcoin's 10 minute cycle, however this is done at the cost of a higher probability of orphaned blocks. This shorter cycle also gives Litecoin greater protection against double spending attacks.

Due to the fact that most altcoins start off as the fork of the Bitcoin project, the vast majority of these altcoins do little in the way of innovating the protocols in place, and as such gain no impactful market share, and are little more that pet projects for interested developers. Some projects do make interesting innovations, and are of interest to the improvement of cryptocurrencies as a whole.

One example of this is Peercoin. While Peercoin shares a large amount of source code with the Bitcoin project, and also has a very similar implementation, it has a very unique feature with the proof-of-stake system that it uses alongside the commonly used proof-of-work system that most altcoins use. Because most altcoins use only a proof-of-work system to process blocks and reward miners, they open themselves up to a potentially economy-destroying flaw.

With only a proof-of-stake system in place, there is potential for a large group of miners to form a coalition, with the possibility to become a monopoly. As they work together, mining difficulty increases, lowering the incentive for new miners to join the network, and creating incentive for existing miners to leave the network, further bringing the coalition closer to having a 51% market share on all mining operations. Once the coalition reaches 51% market share and becomes a monopoly, they could theoretically allow altcoins to be doubly spent, destroying the altcoin's economy.

Peercoin implements its proof-of-stake system in that new coins are generated in a manner that is dependant on the holdings of the individuals involved. This means that if a person in the network is in possession of 5% of the available currency, then they will generate 5% of all proof-of-stake coin blocks. For someone to gain a monopoly similar to how they could in a proof-of-work only system, they would have to be in possession of at least 51% of the crypto-currency, making it for the time being a costly and impractical effort.

Peercoin's design also means that as Peercoin grows, proof-of-stake will become the primary source of coin generation. This has the effect that, relative to the market cap, energy consumption of miners will decrease over time, making it potentially a more energy efficient system. Furthermore, the proof-of-stake contributes with other factors to give Peercoin steady inflation, giving it long term scalability.

VII. Applications of The Blockchain

Ripple is a real-time banking protocol and network that "creates infrastructure solutions that make global financial settlement truly efficient." One of Ripple's overarching goals is to provide an infrastructure for moving value between users utilizing peer-to-peer technologies, like Bitcoin and altcoins do. The way Ripple achieves this by utilizing market makers to allow users to trade value. One such example would be if someone who could only send value in the form of Pesos wanted to send value to someone who could only accept value in the form of Rubles. The ripple network would identify a market maker who holds value in the form of both currencies, and the transaction would be facilitated through this market maker.

The Ripple protocol allows users to essentially post bids for a proposed trade, and the network finds the most efficient path to match trades together. Ripple also has nodes on its network called gateways. Due to the fact that fiat currencies in a digital network have potentially different values (the digital IOU from Bank of America for the physical $100 you deposited is potentially of a different value for the digital IOU you would get from Citibank for the same deposit), Ripple imposes rules that restrict the flow of fiat currencies to entering and exiting the network to specific gateways.

Due to the use of gateways, there is a unique element of trust in the Ripple system. In Bitcoin, while the value of the crypto-currency may vary over time, you will always have that amount. With Ripple, you are essentially making a deposit into the network at a certain gateway, and trusting the network and gateway to either allow you to get your deposit back, whether it is in the same form of your original deposit (i.e. get cash back if you initially deposited cash) or getting items of value from other gateways (i.e. you were able to spend your Ripple deposit on items of value existing outside of the Ripple network, like food).

Ripple also is a network of trust. When you make a deposit at a gateway, you extend trust to it in the Ripple network. You automatically trust that gateway's counter party risk, or trust that the gateway will not default on the debt it owes to you on your deposit. Furthermore, if you make deposits at multiple gateways using the same currency, you can allow rippling to occur, which allows your balance in that currency to switch between the gateways, allowing the ripple network to create more optimal paths for future or pending transactions, and by giving the network inter-gateway liquidity, you gain a transit fee.

While Bitcoin is an entirely decentralized protocol, Ripple has a more permissioned approach, restricting certain operations to taking specific paths through the network, and using more established institutions such as fiat banks to work as entry/exit points, and to hold value in the network. While Bitcoin has huge potential for consumer use in day-to-day transactions, Ripple is seeing a lot of its potential being derived from financial institutions wanting to transfer value between themselves, such as two banks wanting to transfer currency between themselves.

While Ripple is a real-time gross settlement system, Ethereum is an entirely different application of the Blockchain. It is a crypto-currency platform and Turing-complete programming framework intended to allow a network of peers to administer their own user-created smart "contracts" without a central authority. It is also a stateful system, which allows information to be retained over time in the platform. It uses a virtual machine that is derived from the blockchain that securely records and promotes the validation of transactions, where these transactions are actually code executions, made through an Ethereum-specific crypto-currency called Ether. Smart contracts deployed on the Ethereum blockchain are paid for in Ether.

According to its founders: "What Bitcoin does for payments, Ethereum does for anything that can be programmed". It uses its own proof-of-work blockchain and methodology that enables anyone to create these smart contracts that can execute any arbitrary code stored in each block of its blockchain. Ethereum, being a turing complete and entirely programmable system, gives developers on the platform many resources to build anything from decentralized voting systems to crowdfunding platforms. However, it is worth noting that to build these applications on Ethereum you must have Ether, the crypto-currency used for computing on the blockchain.

Another interesting use would be for local governments to use the blockchain to maintain public records. The idea would be to create a hash of a completed form at a particular time. This could be any sort of public record that requires documentation: a marriage certificate, a judge's ruling, or a deed to a property. Then the hash is added to the blockchain. Later, at a time when the document needs to be reviewed, the document can be compared to the hash of the document found on the blockchain to verify that the document has not been altered.

VIII. Conclusion

Bitcoin provides for a means of crypto-currency that does not have to rely on any trusted third parties. Instead it incorporates a peer-to-peer network using a proof of work blockchain to prevent the problem of double spending. We have also seen many other forks of Bitcoin which in their own right provide communities as well for decentralized purchasing. The concept of the Blockchain, the major fundamental breakthrough in computer science that Bitcoin wouldn't work without, is an entirely other revolutionary technology itself. The blockchain, as we have seen here, has applications far beyond crypto-currencies that may one day solve many of the problems we face today. From Ripple to Ethereum, the Blockchain is already changing large financial industries and the world of distributed computing by empowering innovators to build new decentralized applications that before would have never been possible.

References

[Barski] Barski, Conrad and Chris Wilmer. Bitcoin for the Befuddled. San Francisco, CA: No Starch Press, 2015. Print.

[Nakamoto] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System". Nakamotoinstitute.org 31 October 2008.

[Rykwalder] Rykwalder, Eric. "The Math behind Bitcoin". Coindesk.com 19 Oct 2014.

[Kroll] Joshua A. Kroll, Ian C. Davey, Edward W. Felten. "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries". The Twelfth Workshop on the Economics of Information Security (WEIS 2013). June 2013.